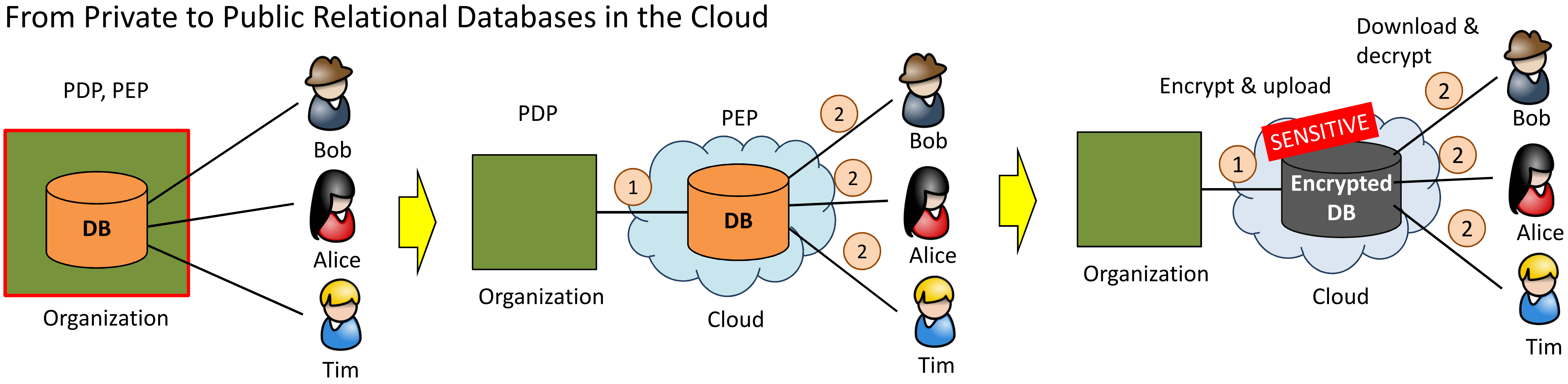
CERIAS

The Center for Education and Research in Information Assurance and Security

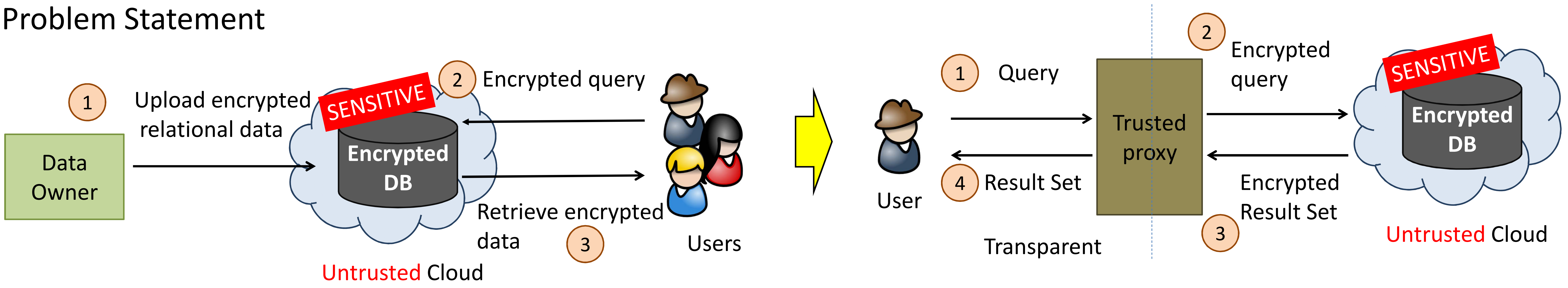
DBMask: Encrypted Query Processing over an Encrypted Database

Mohamed Nabeel, Jianneng Cao, Mohamed Sarfraz, Elisa Bertino
Dept. of Computer Science, Purdue University

From Private to Public Relational Databases in the Cloud



Problem Statement



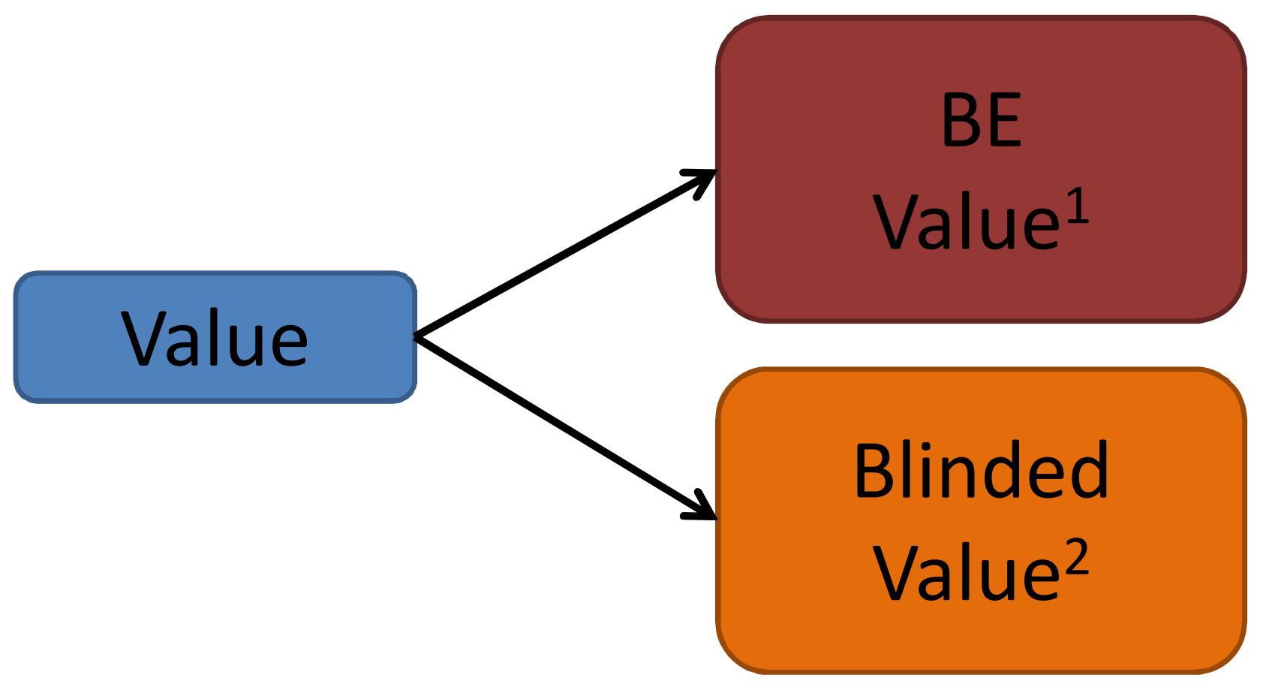
Challenges

(1) How can users **query** and retrieve encrypted data **without the cloud decrypting** the data or query?

(2) How to provide **fine-grained access** to the data over encrypted relational data?

How to support (1) and (2) while allowing **relational database operations**?

Our Approach: SQL Aware Encryption

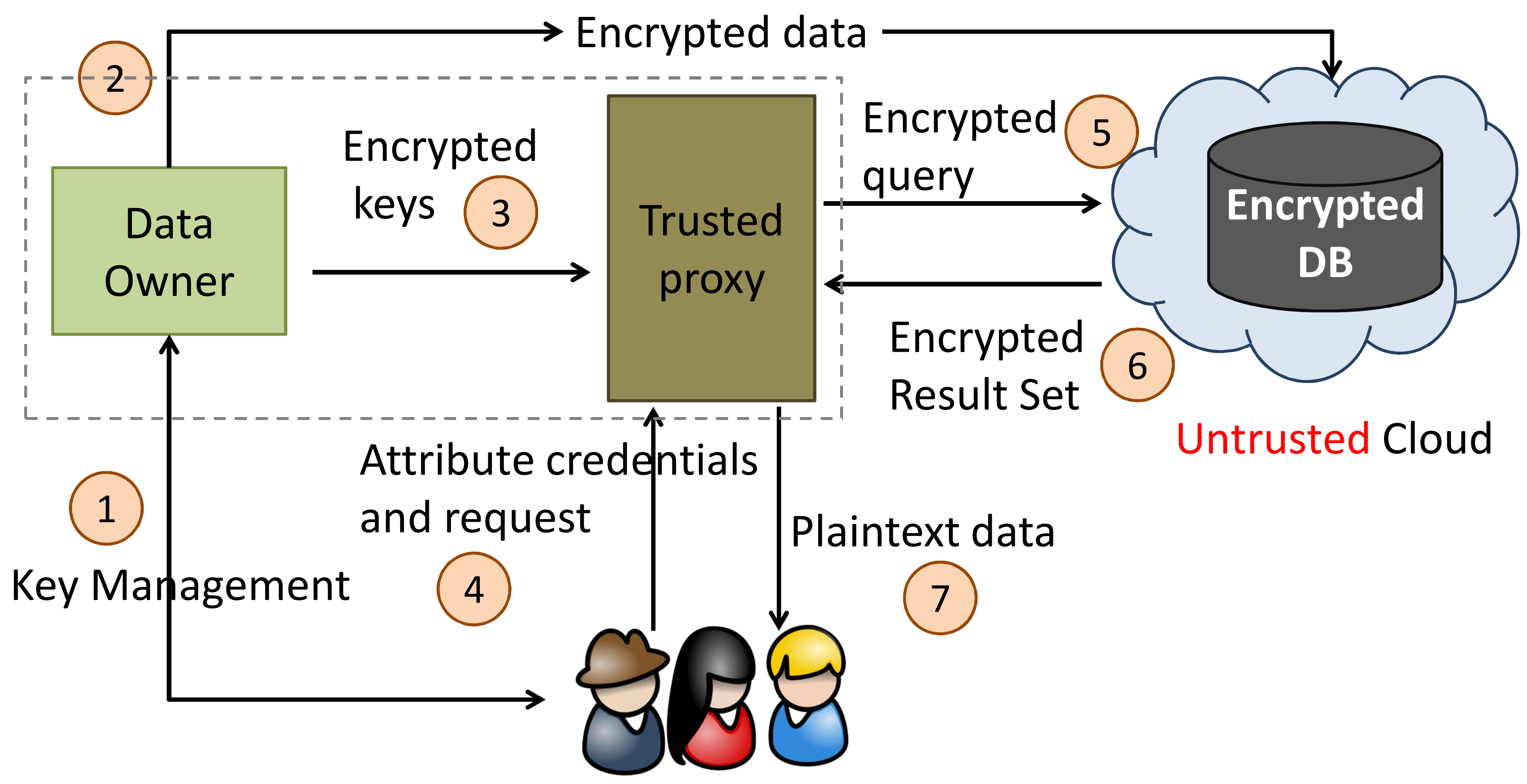


For fine grained (attribute based) access control

For encrypted SQL queries

1. Nabeel et al., Privacy preserving policy based content sharing in the cloud, TKDE 2012
2. Nabeel et al., Efficient privacy preserving publish subscribe systems, SACMAT 2012

Architecture



Example

Patient	Age	Doctor
Alice	15	Sam
Bob	14	Sam
Troy	19	Pat

Access Control Policies:

- A doctor can access only its patients' records
- A patient can access only its record

Sam: SELECT * from Patient WHERE Age > 14;

Patient	BE_Age	B_Age	Doctor	PID
E_{AS}(Alice)	E_{AS}(15)	B(15)	E_{AS}(Sam)	1
E_{BS}(Bob)	E_{BS}(14)	B(14)	E_{BS}(Sam)	2
E_{TP}(Troy)	E_{TP}(19)	B(19)	E_{TP}(Pat)	3

Encrypted table

Proxy: SELECT * from Patient WHERE UDF(B_Age, Trapdoor(14), '>') = 1;

CERIAS
PURDUE UNIVERSITY